

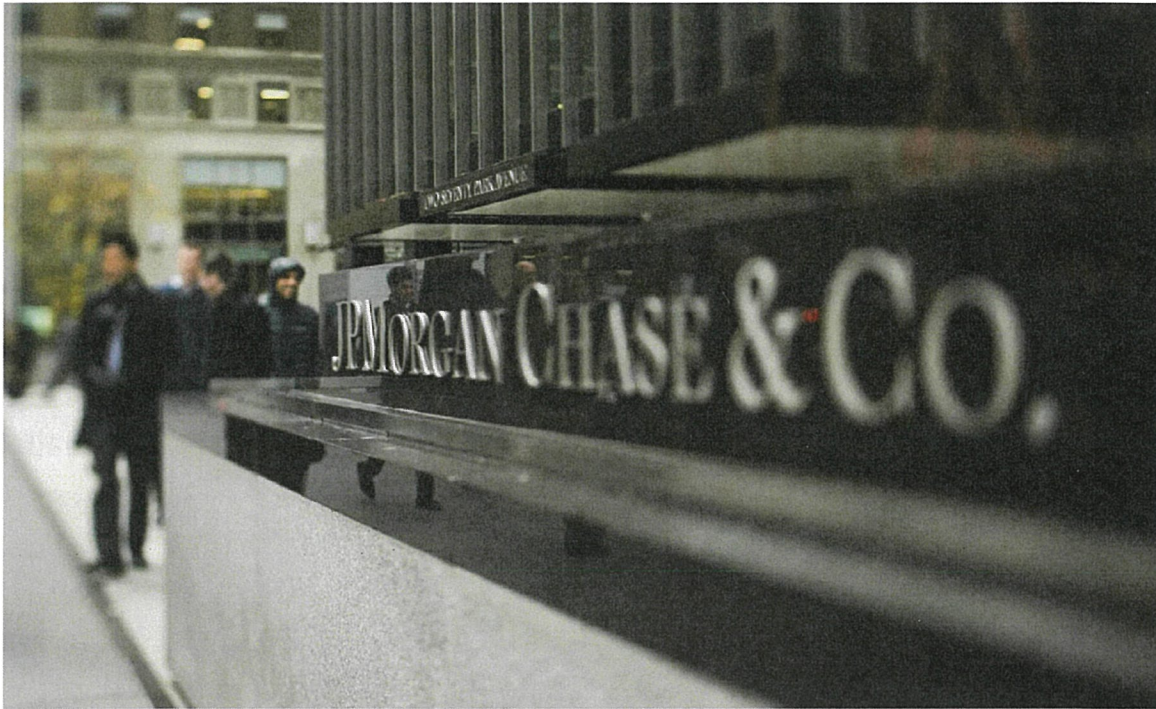
EXHIBIT 5

1/14/25, 12:32 PM

JPMorgan Reassigns Security Team Leader a Year After Data Breach - Bloomberg

Business | Cybersecurity

JPMorgan Reassigns Security Team Leader a Year After Data Breach



JPMorgan Chase & Co. headquarters in New York. *Photographer: Ron Antonelli/Bloomberg*

By Jordan Robertson and Michael Riley

June 30, 2015 at 3:11 PM EDT

 This article is for **subscribers only**.

EXHIBIT 3**Rattray****2/12/2025**

Jessica Waack, CSR
RDR, CRR, NYACR, NYRCR

The executive in charge of protecting JPMorgan Chase & Co.'s computer network from hackers has been reassigned, after a year on the job that included controversy over his handling of a massive data breach and the departure of several top security team members.

Greg Rattray, a former U.S. Air Force commander for information warfare and a cyber-expert at the National Security Council under President George W. Bush, no longer works as JPMorgan's chief information security officer, according to an internal memo sent June 11 and reviewed by Bloomberg News. Rattray is now head of global cyber partnerships and government strategy and reports to Paul Compton, the bank's chief administrative officer.

1/14/25, 12:32 PM

JPMorgan Reassigns Security Team Leader a Year After Data Breach - Bloomberg

Rohan Amin, a former cyber-security executive at Lockheed Martin Corp. who joined JPMorgan last August, has replaced Rattray, according to the memo.

Rattray will oversee a few employees instead of the hundreds he managed in JPMorgan's cyber-security unit, according to a person familiar with the change, one of three people who described events leading up to the personnel move.

One of his responsibilities will be building relationships between the biggest U.S. bank, law enforcement and other government agencies, according to the memo. That move surprised some bank insiders, considering that Rattray's response to the breach discovered last August -- in which hackers stole the names, addresses and e-mail addresses of 83 million individuals and small businesses -- frayed the bank's ties with federal agencies.

Limited Access

Rattray and his boss, Jim Cummings, a former head of the U.S. Air Force's cyber-combat unit, tightly limited access to the breached data in an effort to prevent leaks and control the investigation, Bloomberg Businessweek reported on Feb. 19.

The Secret Service grew so frustrated that it threatened to seize the evidence and Joseph Demarest, then assistant director of the FBI's cyber division, called Chief Operating Officer Matthew Zames to discuss the delays. The situation was resolved with a formal agreement to share information, people familiar with the matter said.

Rattray and Cummings also argued that the attack was probably the work of the Russian government, as they tried to secure a rare waiver from the Justice Department that would have allowed JPMorgan to delay notifying customers and regulators of the loss on national-security grounds. Government investigators quickly concluded that the attack was the work of cyber-criminals, not spies.

Trish Wexler, a JPMorgan spokeswoman, declined to comment on Rattray's reassignment.

1/14/25, 12:32 PM

JPMorgan Reassigns Security Team Leader a Year After Data Breach - Bloomberg

Culture Conflict

Ratray and Cummings are representative of a growing movement among companies to hire former military cyber-warriors to protect private-sector networks. Ratray's sidelining offers a cautionary lesson about the risks of a culture conflict.

The fit was difficult from the start. Some staff members mocked the weekly agenda Ratray sent to them, which he called a "battle rhythm," and Cummings's exhortations to adhere to the Air Force's "core values," such as service to country, in a culture focused on serving clients.

Ratray has an extensive network of contacts and supporters inside the government, including links to the U.S. intelligence community, many of whom have praised his handling of the breach.

"Greg usually knows what he's doing," James Lewis, a senior fellow in cybersecurity at the Center for Strategic and International Studies in Washington, said of him in February.

Internal Battles

Still, his tenure was marked by battles with experienced members of the bank's security team, some of whom agreed that the breach was probably criminal in nature. He also angered some of JPMorgan's technology vendors, who complained that he abruptly canceled contracts and delayed payments on large deals.

Some inside the bank believed the focus on a possible link to the Russian government was an excuse for shortcomings in the bank's security. The hackers entered the bank's network through a server that didn't have strong protections, such as two-factor authentication, which requires a unique code along with a password to gain access.

Others familiar with Ratray's management style, who asked not to be identified when discussing internal matters, said it was the natural result of hiring ex-cyber warriors whose training led them to immediately assume a government link to a sophisticated attack.

1/14/25, 12:32 PM

JPMorgan Reassigns Security Team Leader a Year After Data Breach - Bloomberg

As the largest U.S. bank by assets, JPMorgan has played a major role implementing sanctions against Russian institutions and officials imposed as a result of the conflict in Ukraine.

[Share feedback](#) ☐

©2025 Bloomberg L.P. All Rights Reserved.
